

#2

501.39485X00

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s): OBARA, et al
Serial No.: Not assigned
Filed: March 19, 2001
Title: COMPUTING SYSTEM AND DATA DECRYPTION METHOD
AND COMPUTER SYSTEM WITH REMOTE COPY FACILITY
Group: Not assigned

J1046 U.S. PTO
09/810575
03/19/01

LETTER CLAIMING RIGHT OF PRIORITY

Honorable Commissioner of
Patents and Trademarks
Washington, D.C. 20231

March 19, 2001


Sir:

Under the provisions of 35 USC 119 and 37 CFR 1.55, the applicant(s) hereby claim(s) the right of priority based on Japanese Patent Application No.(s) 2000-155954 filed May 23, 2000 and 2000-271865 filed September 7, 2000 .

Certified copies of said Japanese Application are attached.

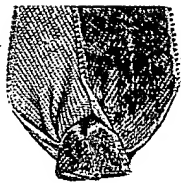
Respectfully submitted,

ANTONELLI, TERRY, STOUT & KRAUS, LLP



Carl I. Brundidge
Registration No. 29,621

CIB/amr
Attachment
(703) 312-6600



日本国特許庁

PATENT OFFICE
JAPANESE GOVERNMENT

J1046 U.S. PTO

09/810575



03/19/01

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日

Date of Application:

2000年 9月 7日

出願番号

Application Number:

特願2000-271865

出願人

Applicant (s):

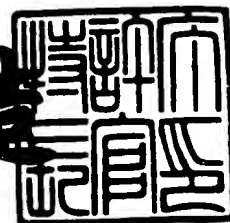
株式会社日立製作所

CERTIFIED COPY OF
PRIORITY DOCUMENT

2000年12月 1日

特許庁長官
Commissioner,
Patent Office

及川耕造



出証番号 出証特2000-3099719

【書類名】 特許願

【整理番号】 KN1126

【提出日】 平成12年 9月 7日

【あて先】 特許庁長官殿

【国際特許分類】 G09C 1/00

【発明者】

 【住所又は居所】 神奈川県小田原市国府津 2 8 8 0 番地 株式会社日立製作所 ストレージシステム事業部内

 【氏名】 高松 久司

【発明者】

 【住所又は居所】 神奈川県小田原市国府津 2 8 8 0 番地 株式会社日立製作所 ストレージシステム事業部内

 【氏名】 野沢 正史

【発明者】

 【住所又は居所】 神奈川県川崎市麻生区王禅寺 1 0 9 9 番地 株式会社日立製作所 システム開発研究所内

 【氏名】 大枝 高

【発明者】

 【住所又は居所】 神奈川県川崎市麻生区王禅寺 1 0 9 9 番地 株式会社日立製作所 システム開発研究所内

 【氏名】 森下 昇

【特許出願人】

 【識別番号】 000005108

 【氏名又は名称】 株式会社 日立製作所

【代理人】

 【識別番号】 100078134

 【弁理士】

 【氏名又は名称】 武 顕次郎

 【電話番号】 03-3591-8550

【手数料の表示】

【予納台帳番号】 006770

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 リモートコピーのコンピュータシステム

【特許請求の範囲】

【請求項 1】 上位装置と接続されてデータの授受を行なう制御手段、前記データの格納を行なう記憶手段、を有するプライマリディスクサブシステム群からなるメインセンターを備え、

前記プライマリディスクサブシステム群と離隔した場所に配置されて前記プライマリディスクサブシステム群から転送される暗号化されたデータを受け取る制御手段、前記転送されたデータの格納を行なう記憶手段、を有するセカンダリディスクサブシステム群からなるリモートセンターを備え、

前記プライマリディスクサブシステム群は、所定の間隔又は不定期の間隔で、暗号鍵を更新するとともに、前記セカンダリディスクサブシステム群への前記データ転送の中断を行い、更新した暗号鍵を前記セカンダリディスクサブシステム群へ転送する

ことを特徴とするリモートコピーのコンピュータシステム。

【請求項 2】 請求項 1 に記載のリモートコピーのコンピュータシステムにおいて、

前記プライマリディスクサブシステム群が前記セカンダリディスクサブシステム群に転送しているデータと同様なデータ長及びデータパターンを持つようなデータを作成し、前記作成したデータに前記暗号鍵を埋め込むことを特徴とするリモートコピーのコンピュータシステム。

【請求項 3】 上位装置と接続されてデータの授受を行なう制御手段、前記データの格納を行なう記憶手段、を有するプライマリディスクサブシステム群からなるメインセンターを備え、

前記プライマリディスクサブシステム群と離隔した場所に配置されて前記プライマリディスクサブシステム群から転送される暗号化されたデータを受け取る制御手段、前記転送されたデータの格納を行なう記憶手段、を有するセカンダリディスクサブシステム群からなるリモートセンターを備え、

前記プライマリディスクサブシステム群は、データの書込処理の実行中に暗号

化したデータ転送の暗号鍵を更新するタイミングであるか否かを判断し、更新タイミングであれば、前記暗号鍵を更新するとともに前記更新した暗号鍵に順序番号を付加して前記セカンダリサブシステムに転送し、順序番号の付加された転送データと対応付けする

ことを特徴とするリモートコピーのコンピュータシステム。

【請求項4】 請求項1又は3に記載のリモートコピーのコンピュータシステムにおいて、

前記プライマリディスクサブシステム群から前記セカンダリディスクサブシステム群に暗号化して転送されたデータを、復号することなく前記リモートセンターの記憶手段に保存し、災害回復のタイミングで復号する

ことを特徴とするリモートコピーのコンピュータシステム。

【請求項5】 請求項4に記載のリモートコピーのコンピュータシステムにおいて、

前記プライマリディスクサブシステム群から前記セカンダリディスクサブシステム群にデータを暗号化して転送する際に、前記暗号鍵を前記リモートセンターとは別地に配置された他のリモートセンターにリモートコピーして保存し、災害回復のタイミングで前記他のリモートセンターに保存された暗号鍵を使用してデータ復号する

ことを特徴とするリモートコピーのコンピュータシステム。

【請求項6】 請求項4に記載のリモートコピーのコンピュータシステムにおいて、

前記プライマリディスクサブシステム群から前記セカンダリディスクサブシステム群に暗号化して転送されたデータを復号する際に、前記データに関するレコードの特定部分を搜索した場合にのみ復号する

ことを特徴とするリモートコピーの暗号化システム。

【請求項7】 請求項1又は3に記載のリモートコピーのコンピュータシステムにおいて、

前記プライマリディスクサブシステム群と前記セカンダリディスクサブシステム群との間は、ストレージエリアネットワークを経由して接続されていることを

特徴とするリモートコピーのコンピュータシステム。

【請求項 8】 請求項 1 又は 3 に記載のリモートコピーのコンピュータシステムにおいて、

前記プライマリディスクサブシステム群と前記セカンダリディスクサブシステム群との間のデータ転送は、同期形転送又は非同期形転送で行なうことを特徴とするリモートコピーのコンピュータシステム。

【請求項 9】 上位装置に接続されて前記上位装置からデータの転送を受けるプライマリディスクサブシステム群からなるメインセンターと、前記メインセンターの前記プライマリディスクサブシステム群と接続されてデータの転送を受けるセカンダリディスクサブシステム群からなるリモートセンターと、から構成され、

前記プライマリディスクサブシステム群は、前記セカンダリディスクサブシステム群にデータをリモートコピーする際に暗号化してデータ転送するか否かを規定した制御情報を格納したリモートコピー制御情報格納部を有し、前記制御情報が暗号化してデータ転送すると規定している場合にデータの暗号化を行ない、

前記セカンダリディスクサブシステム群は、前記プライマリディスクサブシステム群の前記制御情報を確認し、前記制御情報が暗号化してデータ転送するとなっている場合に転送されたデータに対して暗号化に適應した処理を行なう

ことを特徴とするリモートコピーのコンピュータシステム。

【請求項 10】 上位装置から書込まれるデータを記憶するローカル側記憶システムと、前記データのコピーを記憶するリモート側記憶システムから構成される記憶システムのリモートコピー方法であって、

前記ローカル側記憶システムが前記データを暗号鍵で暗号化するステップと、

前記ローカル側記憶システムから前記リモート側記憶システムシステムへ、前記暗号化したデータを転送するステップと、

前記暗号鍵を繰り返し更新するステップと、

前記更新した暗号鍵を、前記ローカル側記憶システムから前記リモート側記憶システムへ転送するステップと、を有し、

前記暗号化するステップは、前記暗号鍵が更新された後は更新後の暗号鍵を使

用する

ことを特徴とする記憶システムのリモートコピー方法。

【請求項 1 1】 請求項 1 0 に記載の記憶システムのリモートコピー方法の
いて、

前記暗号鍵を更新するステップの繰り返しの頻度は、当該暗号鍵を解読する時
間から決められることを特徴とする記憶システムのリモートコピー方法。

【発明の詳細な説明】

【 0 0 0 1 】

【発明の属する技術分野】

本発明は、コンピュータシステムのデータを格納する外部記憶装置及びこれら
の統合システムに関し、特に、複数の外部記憶装置（サブシステム群）と遠隔地
に存在する他の複数の外部記憶装置（サブシステム群）とを相互に接続し、遠隔
地に存在する外部記憶装置（サブシステム群）の間でデータを二重化するリモ
ートコピー技術において、データを暗号化して転送する技術に関する。

【 0 0 0 2 】

【従来の技術】

地震等の天災の際のデータのバックアップを考慮すれば、ホストコンピュータ
（上位装置）とサブシステム等から構成されるセンターにおいて、メインセンタ
ーとリモートセンターは数 1 0 0 k m 程度、分離する必要がある。ここで、サブ
システムとは、上位装置に対して情報の授受を行なう制御部と、情報の格納を行
なうディスク装置等を内蔵する記憶装置を言う（記憶装置がディスク装置の場合
はディスクサブシステムと称する）ものである。このため、メインセンターとリ
モートセンターにそれぞれ設置されているサブシステムの間で、データを二重化
して保有する、いわゆる、リモートコピー機能を採用した外部記憶システムが、
既にいくつか実用化されている。

【 0 0 0 3 】

リモートコピー機能は、同期形と非同期形の 2 種類に大別される。同期形とは
メインセンター内のホストコンピュータ（上位装置）からメインセンター内のサ
ブシステムに、データの更新（書き込み）指示が有った場合、その指示対象がリモ

ートコピー機能の対象でもあるときは、そのリモートコピー機能の対象であるリモートセンターにおけるサブシステムに対して、指示された更新（書き込み）が終了してから、メインセンターの上位装置に更新処理の完了を報告する処理手順をいう。この場合、メインセンターとリモートセンターとの地理的距離に応じて、この間に介在するデータ伝送線路の能力の影響を受け、時間遅れ（伝送時間等）が発生する。

【0004】

これに対して、非同期形とは、メインセンター内の上位装置からサブシステムにデータの更新（書き込み）指示があった場合、その指示対象がリモートコピー機能の対象であっても、メインセンター内のサブシステムの更新処理が終わり次第、上位装置に対して更新処理の完了を報告し、リモートセンターのサブシステムにおけるデータの更新（反映）はメインセンターにおける処理とは非同期に実行する処理手順をいう。このためメインセンター内部で必要とされる処理時間でデータ更新が終了するので、リモートセンターへのデータの格納に起因する伝送時間等はかからない。

【0005】

非同期形は、リモートセンターのサブシステムの内容が、メインセンター側のそれに対して、常に一致しているわけではない。このため、メインセンターが災害等により機能を失った場合は、リモートセンター側にデータの反映が完了していないデータが消失することとなる。しかし、メインセンター側のサブシステムのアクセス性能を、リモートコピー機能を実施しない場合と同等レベルとすることが出来る。

【0006】

これらのリモートコピー機能を遠隔地間で高性能かつ廉価に実現するには、非同期形を使用することになる。この場合、メイン側からリモート側へデータを転送（コピー）する伝送路として公衆通信回線を使用することになるため、以下に記述するような、情報の漏洩防止が重要な課題となる。

【0007】

「暗号化したデータ転送について」

公衆通信回線を経由したデータ転送を行なう場合、情報の漏洩防止のため、暗号化したデータ転送が行なわれており、これをリモートコピーに適用することが考えられる。この場合、メインセンターのプライマリディスクサブシステム群とリモートセンターのセカンダリディスクサブシステム群との間で暗号化したデータ転送を行なう事になる。リモートコピーにおいては、長期間にわたってデータ転送を行なう為、高いデータ転送性能と高い暗号強度を両立させなければならない。

【0008】

「通信路における暗号化したデータ転送について」

ネットワーク経由でデータを通信する2台以上のコンピュータを備えたデータ通信システムにおいて、自己のコンピュータのアプリケーションプログラムが他方のコンピュータのアプリケーションプログラムに対して、データを暗号化して送信する方式がある。この方式の具体的開示は、例えば「暗号化データ通信システム」として、特開平9-139735号公報に詳細になされている。前記「暗号化データ通信システム」においては、2台のコンピュータ上で、それぞれ中継サービスプログラムを動作させておき、この中継サービスでデータを暗号化してネットワーク経由で送受信することにより通信路における暗号化したデータ転送を実現している。

【0009】

【発明が解決しようとする課題】

従来技術（暗号化データ通信システム）により、通信路における暗号化したデータ転送の機能が実現出来る。しかし従来技術では、長期間にわたってデータ転送を行なう場合、同一の暗号鍵を長時間更新することなく用いているので、暗号鍵が悪意に解読されデータが盗まれる虞があった。また、暗号鍵を更新するにしてもオフラインで通知していたので、データ転送性能が悪くなっていた。即ち、従来技術では、高いデータ転送性能と高い暗号強度との両立が考慮されていない。

【0010】

本発明の目的は、高いデータ転送性能と高い暗号強度とを両立させたりリモート

コピー機能を実現することである。

【 0 0 1 1 】

【課題を解決するための手段】

前記課題を解決するために、本発明は主として次のような構成を採用する。

【 0 0 1 2 】

上位装置と接続されてデータの授受を行なう制御手段、前記データの格納を行なう記憶手段、を有するプライマリディスクサブシステム群からなるメインセンターを備え、

前記プライマリディスクサブシステム群と離隔した場所に配置されて前記プライマリディスクサブシステム群から転送される暗号化されたデータを受け取る制御手段、前記転送されたデータの格納を行なう記憶手段、を有するセカンダリディスクサブシステム群からなるリモートセンターを備え、

前記プライマリディスクサブシステム群は、所定の間隔又は不定期の間隔で、暗号鍵を更新するとともに、前記セカンダリディスクサブシステム群への前記データ転送の中断を行い、更新した暗号鍵を前記セカンダリディスクサブシステム群へ転送するリモートコピーのコンピュータシステム。

【 0 0 1 3 】

また、上位装置と接続されてデータの授受を行なう制御手段、前記データの格納を行なう記憶手段、を有するプライマリディスクサブシステム群からなるメインセンターを備え、

前記プライマリディスクサブシステム群と離隔した場所に配置されて前記プライマリディスクサブシステム群から転送される暗号化されたデータを受け取る制御手段、前記転送されたデータの格納を行なう記憶手段、を有するセカンダリディスクサブシステム群からなるリモートセンターを備え、

前記プライマリディスクサブシステム群は、データの書込処理の実行中に暗号化したデータ転送の暗号鍵を更新するタイミングであるか否かを判断し、更新タイミングであれば、前記暗号鍵を更新するとともに前記更新した暗号鍵に順序番号を付加して前記セカンダリサブシステムに転送し、順序番号の付加された転送データと対応付けするリモートコピーのコンピュータシステム。

【 0 0 1 4 】

また、上位装置から書込まれるデータを記憶するローカル側記憶システムと、前記データのコピーを記憶するリモート側記憶システムから構成される記憶システムのリモートコピー方法であって、

前記ローカル側記憶システムが前記データを暗号鍵で暗号化するステップと、

前記ローカル側記憶システムから前記リモート側記憶システムシステムへ、前記暗号化したデータを転送するステップと、

前記暗号鍵を繰り返し更新するステップと、

前記更新した暗号鍵を、前記ローカル側記憶システムから前記リモート側記憶システムへ転送するステップと、を有し、

前記暗号化するステップは、前記暗号鍵が更新された後は更新後の暗号鍵を使用する記憶システムのリモートコピー方法。

【 0 0 1 5 】

【発明の実施の形態】

本発明の実施形態に係るリモートコピーのコンピュータシステムについて図面を用いて以下説明する。図 1 は本発明の実施形態に係るリモートコピーのコンピュータシステムの全体構成を示す図であり、図 3 は本実施形態に関するメインセンターのプライマリディスクサブシステムの具体的構成を示す図である。

【 0 0 1 6 】

図 1 に、コンピュータシステムを装備した複数のデータセンターにおいて、任意の 2 つのセンター間で情報（データ）の二重化を行なうため、本発明の一実施形態を適用したときの構成例を示す。

【 0 0 1 7 】

メインセンター 9 側の一台又は複数台のディスクサブシステム 3（3-1、3-2、…、3-n）と、リモートセンター 10 側の一台又は複数台のディスクサブシステム 7（7-1、7-2、…、7-n）は、上位装置（ホストコンピュータ）1、8 を介さずに接続され、両センター間でデータの二重化を行なうリモートコピーシステムを実現している。上位装置を介さないディスクサブシステムの接続としては、例えば、SAN（Storage Area Network）が

挙げられる。図3にメインセンター9のディスクサブシステム3の構成例を示す。

【0018】

図1のメインセンター9において、データ処理を行なう中央処理装置（CPU）を持つ上位装置1は、伝送経路であるインタフェースケーブル2を介して、プライマリディスクサブシステム3-1、3-2、……3-nに接続されている。

【0019】

プライマリディスクサブシステム3-1、3-2、……3-nは、図3に示すように、上位装置1からのデータ（情報を含む）授受を行なうインタフェース制御部21と、上位装置1から参照又は更新されるデータ及びリモートコピーが一次停止中の更新データの格納位置に関する情報を格納するデータバッファ22と、このデータを記録する記録媒体としての磁気ディスクドライブ23と、これらのデータのやり取りを制御するマイクロプロセッサ24と、これらの各要素を制御するディスクアレイサブシステム制御部25と、を備える。なお、インタフェース制御部21はリモートセンター10との間でデータ授受を行うインタフェースでもある。

【0020】

また、プライマリディスクサブシステム3-1は、上述した構成要素群に加えて、リモートコピーをどのような設定にて行なうかをユーザが設定するコンソール26と、コンソール26により設定された制御情報により現在のリモートコピー状況を表わす制御ビットを格納するリモートコピー制御情報格納部27と、を備える。

【0021】

メインセンター9のプライマリディスクサブシステム3-1は、インタフェースケーブル4-1を介してリモートセンター10のセカンダリディスクサブシステム7-1と接続される。同様に、プライマリディスクサブシステム3-2は、インタフェースケーブル4-2を介して、セカンダリディスクサブシステム7-2と接続され、プライマリディスクサブシステム3-nは、インタフェースケー

ブル4-nを介して、リモートセンタのセカンダリディスクサブシステム7-nと接続される構成をとる。

【0022】

なお、インタフェースケーブル4-1、4-2、……4-nは、回線接続装置等を利用して一般の公衆通信回線と接続することも可能である。本構成例ではこの点も含めてインタフェースケーブル4-1～4-nとして記述する。

【0023】

また、ディスクサブシステム3が複数台有る場合には、ディスクサブシステム3-1は、メインセンター9内でリモートコピー対象のデータが格納されるディスクサブシステム3-1以外のディスクサブシステム3-2、……3-nとインタフェースケーブル5を介して接続されている。この様に、メインセンター9側ではリモートコピー対象のデータが格納されるディスクサブシステム3-1について、プライマリディスクサブシステム群3全体がインタフェースケーブル5で接続される構成をとる。

【0024】

プライマリディスクサブシステム群3は、上位装置1がプライマリディスクサブシステム群3にデータの書込要求を発行すると、これに同期して当該データを自己のサブシステム内のデータバッファ22に書き込み、更に自己のサブシステム内のデータバッファ22にデータが書き込まれたこととは非同期に、遠隔地に存在するセカンダリディスクサブシステム群7に対して、データの書込指示を行なうディスクサブシステム群である。自己のサブシステム内のデータバッファ22に書き込まれた当該データは、同期或いは非同期にて磁気ディスクドライブ23に記録される。

【0025】

遠隔地に非同期形でデータを書込むリモートコピーの方法として、メインセンター9のプライマリディスクサブシステム群3は、自己のサブシステム内のボリュームが更新された順番に従い、自サブシステムが接続されているリモートセンター10のセカンダリディスクサブシステム群7に更新データを転送して、リモートセンター10のセカンダリディスクサブシステム群7は受取った順番に従い

、更新データを自己のサブシステム内のボリュームに反映するモードと、メインセンター 9 側が自己のサブシステム内のボリュームが更新された順番によらずにプライマリディスクサブシステム群 3 で最適にスケジューリングされた契機で転送対象のデータを纏めて転送して、リモートセンター 10 のセカンダリディスクサブシステム群 7 は受取った順番に関係なく更新データを更新された順番で自己のサブシステム内のボリュームに反映するモードと、を保有する。

【 0 0 2 6 】

セカンダリディスクサブシステム群 7 は、インタフェースケーブル 4 により接続されたプライマリディスクサブシステム群 3 からインタフェース制御部 2 1 経由で受取ったデータを自サブシステム内のデータバッファ 2 2 に格納する。

【 0 0 2 7 】

つまり、上位装置 1 から一台または複数台のディスクサブシステム 3 - 1、3 - 2、…… 3 - n に対しデータの書き込み指示があった場合には、リモートセンター 10 内の一台または複数台のディスクサブシステム 7 - 1、7 - 2、…… 7 - n にも同じデータが格納されるシステム構成を示している。図 1 の矢印は、上位装置 1 から書き込み指示のあったデータの流れを示している。

【 0 0 2 8 】

なお、プライマリディスクサブシステム群 3 は、リモートコピーにおける暗号化の状態を表わす制御ビットをリモートコピー制御情報格納部 2 7 内に持っており、予めシステム運用者により設定された契機もしくは不定期間隔の契機もしくは任意の時点でのシステム運用者による指示に基づき、この制御ビットの情報を変更することによってリモートコピーを一時停止状態にすることができる。なお、本発明の一実施形態では、この一時停止状態に、更新した暗号鍵をプライマリ側からセカンダリ側へ通知することになる（詳細は後述）。リモートコピーが一時停止のときは、プライマリディスクサブシステム群 3 はセカンダリディスクサブシステム群 7 への更新データの書き込み指示の発行は行なわずに保留する。

【 0 0 2 9 】

ここで、プライマリディスクサブシステム 3 - 1 のリモートコピー制御情報格納部には、前記セカンダリディスクサブシステム群にデータをリモートコピーす

る際に暗号化してデータ転送するか否かを規定した制御情報を格納しても良い。前記制御情報が暗号化してデータ転送すると規定している場合にデータの暗号化を行なってデータ転送すると共に、一方、前記セカンダリディスクサブシステム群では、前記プライマリディスクサブシステム群の前記制御情報を確認し、前記制御情報が暗号化してデータ転送となっている場合に転送されたデータに対して暗号化に適応した処理を行なうことで（例えば、暗号鍵を用いて転送データを復号するように対処すること）、メインセンターからリモートセンターへコピーされたデータの整合性を取ることができる。

【 0 0 3 0 】

本発明では、このようにリモートコピーを一時停止させ、この間に更新した暗号鍵をリモートセンターへ通知することによりメインセンター 9 側のデータとリモートセンター 1 0 側のデータとで使用される暗号鍵の整合性を取ることが出来るので、上位装置の介在無しでリモートコピーの暗号鍵の更新を実現することが出来る。このためメインフレームだけでなくオープン系のシステムであっても、同様の機能を実現することが出来る。

【 0 0 3 1 】

また、プライマリディスクサブシステム群 3 は、予めシステム運用者により設定された契機もしくは不定期間隔の契機もしくは任意の時点でのシステム運用者による指示に基づき、上記一時停止状態を解除することが出来る。

【 0 0 3 2 】

一時停止状態が解除されると、プライマリディスクサブシステム群 3 は、上位装置 1 からプライマリディスクサブシステム群 3 ヘデータの書込要求が発行された場合は、これに同期して当該データを自己のサブシステム内のデータバッファ 2 2 に書き込み、更に、自己のサブシステム内のデータバッファ 2 2 にデータが書き込まれたこととは非同期に、遠隔地に存在するセカンダリディスクサブシステム群 7 に対してデータの書込指示を行なう。そして、実際にリモートセンターヘデータを転送する際に更新した暗号鍵を用いる。

【 0 0 3 3 】

このような構成とする事により、メインセンター 9 内のリモートコピー対象の

プライマリディスクサブシステム群3のボリュームと、リモートセンター10内のセカンダリディスクサブシステム群7のボリュームとにおいて、同一のタイミングで暗号鍵の更新が出来る。さらに、プライマリディスクサブシステム群3においてリモートコピーが一時停止状態となっている間は、プライマリディスクサブシステム群3が一時停止状態となった時点のメインセンター9のプライマリディスクサブシステム群3のデータの状態と、リモートセンター10のセカンダリディスクサブシステム群7でのデータの状态とが一致している。即ち当該時点で2センター間で一貫性が保証されたデータの状态が保証・維持される。

【0034】

なお、リモートコピーの一時停止や一時停止の解除は、リモートコピーのボリュームペア単位に設定出来る。複数のボリュームペアを一つのボリュームグループに設定して、ボリュームグループ単位に状態を変化させることも可能である。そして、一時停止や一時停止解除を何れかのサブシステム3, 7や上位装置1, 8のコンソール、或いはこれらのシステムを管理する際に使用するモニターに表示することによって、ユーザはリモートコピーが現在行なわれているか否か、またどのような単位でリモートコピーが行われているかを認識する事が出来る。

【0035】

このリモートコピーの一時停止及び一時停止解除の間隔はユーザの任意に設定する事が可能である。ここではリモートコピーの転送データの傍受による暗号解読の危険性の高まりに要する時間を周期として、メインセンター9からリモートセンター10へのリモートコピーを行い、ここで一時停止して、更新された暗号鍵を送信して、その後に一時停止を解除して、再びリモートコピーを行なうというサイクルを挙げておく。勿論、この例に囚われずに一時停止及び一時停止解除の間隔を設定しても良い。

【0036】

上位装置8は、リモートセンター10においてセカンダリディスクサブシステム群7とインタフェースケーブル6によって接続され、セカンダリディスクサブシステム群7に対して、参照及び更新を行なう中央処理装置である。上位装置8は、メインセンター9の上位装置1が災害や故障等により本来の機能を果たせない

くなった場合に、上位装置 1 の代替となって処理を行なうことが出来る。このほか、セカンダリディスクサブシステム群 7 に格納されているデータを使用して、メインセンター 9 の上位装置 1 とは異なる処理を、上位装置 1 とは別個独立に実行することが出来るものである。

【 0 0 3 7 】

但し、上位装置 8 がセカンダリディスクサブシステム群 7 に対して処理を行わない場合や上位装置 1 の代替機能を備えない場合には、上位装置 8 は不要である。逆に、上位装置 8 を備え、ディスクサブシステム 7-1 を他のディスクサブシステム 7-2 ~ 7-n とインタフェースケーブル 11 で接続し、メインセンター 9 のプライマリディスクサブシステム群 3 と同様の構成とすることで図 1 のメインセンター 9 をリモートセンターとして、リモートセンター 10 をメインセンターとして機能させることも可能である。

【 0 0 3 8 】

本発明の実施形態として、データの二重化方法と運用を図 2 を用いて説明する。

【 0 0 3 9 】

二重化の対象となるデータが格納されたファイルやボリューム、ディスクサブシステム 3 は、事前に運用者が二重化つまりリモートコピーの必要に応じて選択する。そして、対象ファイルや対象ボリューム及びディスクサブシステム 3 と、選択したデータの複製を格納するファイルやボリューム及びディスクサブシステム 7 との関係や、二重化する際に更新順序の整合性を常時保持する必要が有るか否かを、予め運用者が上位装置 1 或いはコンソール 26 等からプライマリディスクサブシステム 3-1 内のリモートコピー制御情報格納部 27 に対し設定しておく。

【 0 0 4 0 】

また、プライマリディスクサブシステム 3-1 については、リモートコピーを一時停止させる契機並びに一時停止を解除する契機を設定する。契機の設定は、上位装置 1 から指示できるため、運用の自動化を支援する上位装置 1 のプログラムにより上位装置 1 からの指示契機を予めスケジューリングしておくことが可能

である。

【 0 0 4 1 】

上記の選択、設定に際し、専用のコンソール 2 6 を接続又は装備できるディスクサブシステム 3 の場合には、上位装置 1 を利用せず、そのコンソール 2 6 を通じて設定できる。本例では、上位装置 1 を利用せず、プライマリディスクサブシステム群 3 内部で保有する時間値を利用して、予め運用者がプライマリディスクサブシステム 3 - 1 において、不定期間隔でリモートコピーの一時停止、並びに一時停止の解除が実施されるように設定しておく。

【 0 0 4 2 】

図 2 のフローは専用のコンソールから選択・設定を行なう場合を示している。リモートコピーのパスやボリュームペアの初期設定、即ちどのディスクサブシステムにリモートコピー要求を出すかの設定は、ユーザが予め上位装置 1 に対して設定しておく（ステップ 1：図では S 1 の様に示す。以下同じ）。また、リモートコピーの一時停止や一時停止解除の初期設定は、リモートコピー対象のボリュームペア単位に設定する（ステップ 2）。通常は、リモートコピー対象のボリュームペアすべてを一つのボリュームグループとして定義し、ボリュームグループ内のボリュームはすべて同一のステータスとなるように設定する。

【 0 0 4 3 】

本例では、ディスクサブシステム 3 のボリューム全てをリモートコピー対象とする。従って、以下では、リモートコピーの状態を、ボリュームペアやボリュームグループ単位ではなく、ディスクサブシステム単位として記述する。

【 0 0 4 4 】

リモートコピー対象のファイルやボリュームの設定方法としては、ボリュームやディスクサブシステムを意味する具体的なアドレスを指定する方法や、ディスクサブシステム内の制御プログラムによって、アドレスの任意の範囲から選択する方法を取ることにもできる。初期設定として、パスやボリュームペアの設定、並びに一時停止契機や一時停止解除契機の設定を行なう例を示してある。

【 0 0 4 5 】

上位装置 1 から、プライマリディスクサブシステム 3 - 1、3 - 2、……、

3-n に対し、ライトコマンドが発行されると（ステップ3）、プライマリディスクサブシステム3-1、3-2、……、3-n はライトコマンドに基づき自己のディスクサブシステム内のデータバッファ22へのデータ格納処理を実行する（ステップ4）。ここで、ライトコマンドとは、データを書込むための指示と書込みデータそのものを転送するコマンドである。

【0046】

ライトコマンドを受領した際、プライマリディスクサブシステム3-1、3-2、……、3-n は、プライマリディスクサブシステム群3のリモートコピー制御情報格納部27に格納されているリモートコピー状態を表す制御ビットを取得・参照することにより、プライマリディスクサブシステム群3がリモートコピー一時停止状態にあるか否かを確認する（ステップ5）。プライマリディスクサブシステム3-1、3-2、……3-n はプライマリディスクサブシステム群3がリモートコピー一時停止状態にある場合、データバッファ22へのデータ書き込みが終了すれば上位装置1に対しライトコマンドに対する処理の完了を報告する（ステップ6）。この後、ライトコマンドをセカンダリディスクサブシステム7-1、7-2、……7-n に対し発行し、ライトコマンドに対する処理を完了させる。

【0047】

なお、メインセンタにおいて以前に更新が行なわれたデータについて、リモートセンタに未転送のデータの格納位置情報を保持している場合は、当該位置の全てのデータもリモートセンタのセカンダリディスクサブシステム7-1、7-2、……7-n への転送対象と判断し、当該データを書込む為のライトコマンドをセカンダリディスクサブシステム7-1、7-2、……7-n に対し発行し、ライトコマンドに対する処理を完了させる。この際、現在、設定されている暗号鍵を用いて、データを暗号化して、プライマリディスクサブシステムからセカンダリサブシステムへ転送する。即ち、当該書込みコマンドによるデータ及び未転送の全ての更新データ（書込みデータ）は、現在の暗号鍵により暗号化され、リモートセンタへ全て転送される（ステップ7）。その後、データ転送は一時停止状態になる。

【0048】

次に、メインセンタ内の暗号鍵（暗号鍵はこれを用いてデータを暗号化／復号化するためのもの）を更新する（ステップ8）。この後、更新された暗号鍵をセカンダリディスクサブシステム7-1、7-2、……7-nに転送する（ステップ9）。暗号鍵を転送後、プライマリディスクサブシステム3-1、3-2、……3-nはプライマリディスクサブシステム群3のリモートコピー（データ転送）一時停止状態を解除する（ステップ10）。従って、リモートコピー一時停止状態後は、更新された新しい暗号鍵が使用される。つまり、リモートへ転送されるデータは新しい暗号鍵（更新された暗号鍵）で暗号化され、この暗号化されたデータがリモートへ転送される。

【0049】

なお、ステップ8及びステップ9においては、プライマリディスクサブシステム群3からセカンダリディスクサブシステム群7に一般的に転送しているデータと同様のデータ長／データパターンを持ったデータを作成し、その一部として更新した暗号鍵を埋込み、暗号鍵をリモートへ転送しても良い。こうすることによって、暗号鍵を転送する特別なパケットを使用する必要が無くなり、且つ、外部からは、一般データと思えるため、リモートコピーの一時停止のタイミングを外部から隠蔽することが可能となり、結果として暗号化議を送る際の安全性が高くなる。ここで暗号鍵を埋め込むべきデータは一般に転送しているデータに似せることが重要であり、必ずしも完全に一致させる必要はない。

【0050】

一方、ステップ5でプライマリディスクサブシステム群3がリモートコピー一時停止状態にない場合は、プライマリディスクサブシステム3-1、3-2、……、3-nは、データバッファ22へのデータ書き込みが終了すれば上位装置1に対しライトコマンドに対する処理の完了を報告し（ステップ11）、自己のサブシステムの処理能力に基づいて決定された契機で、ライトコマンドをセカンダリディスクサブシステム7-1、7-2、……7-nに対し発行する。この時メインセンタにおいて更新（書込み）が行なわれたデータについて、リモートセンタにライトコマンドが直ちに発行されない場合があるが、これはリモートセ

ンタへ未転送のデータの格納位置情報として自サブシステム内に保持しておく。
また、メインセンタにおいて以前に更新が行なわれたデータについて、リモートセンタに未転送のデータの格納位置情報を保持している場合は、当該位置のデータもリモートセンタのセカンダリディスクサブシステム7-1、7-2、……7-nへの転送対象と判断し、当該データを書込む為のライトコマンドを発行する。この際、現在用いている暗号鍵を用いて暗号化してセカンダリへ転送する（ステップ12）。当該データの格納位置情報は、ライトコマンドに対するリモートへの転送処理が完了した後に、これを消去する。

【0051】

即ち、プライマリディスクサブシステム群3がリモートコピー一時停止状態にあれば、メインセンタ9のプライマリディスクサブシステム群3は、暗号鍵を更新すると共に更新された暗号鍵をリモートセンタ10のセカンダリディスクサブシステム群7に転送する。また、プライマリディスクサブシステム群3がリモートコピー一時停止状態になれば、メインセンタ9のプライマリディスクサブシステム群3は上位装置1からライトコマンドが発行される事に起因し現在の暗号鍵を用いてリモートコピーが実施される。

【0052】

セカンダリディスクサブシステム7-1、7-2、……7-nは、プライマリディスクサブシステム3-1、3-2、……3-nから発行されたライトコマンドを受領していることを確認すると、ライトコマンドに対する処理、即ち、自己のサブシステム内のデータバッファ22へのデータ格納処理を行なう（ステップ13）。

【0053】

セカンダリディスクサブシステム7-1、7-2、……7-nは、ライトコマンドに対する処理、即ち、自己のサブシステム内のデータバッファ22へのデータ格納処理が完了すると、プライマリディスクサブシステム3-1、3-2、……3-nに対し、ライトコマンドに対する処理完了報告を行なう（ステップ14）。

【0054】

本発明により、上位装置 1 から書込まれたデータは、プライマリディスクサブシステム 3-1、3-2、……、3-n に格納されるだけでなく、セカンダリディスクサブシステム 7-1、7-2、7-n にも複写され格納される。また、プライマリディスクサブシステム群 3 がリモートコピー一時停止状態となった時点のプライマリディスクサブシステム 3-1、3-2、……3-n のデータの状態が、リモートセンタ 10 側のセカンダリディスクサブシステム 7-1、7-2、……7-n で生成される。この時、プライマリディスクサブシステム群 3 が更新された暗号鍵をセカンダリディスクサブシステム群 7 に転送する。

【0055】

セカンダリディスクサブシステム群 7 は、プライマリディスクサブシステム群 3 によって更新された暗号鍵を受取った時点から、当該更新された暗号鍵を使用してデータを復号することが出来る。メインセンタ 9 が被災した場合は、セカンダリディスクサブシステム 7-1、7-2、……7-n のデータを利用して、ジョブを再実行する等の回復作業を行ない、業務を再開する。これらはすべてディスクサブシステムの機能のみで実現され、上位装置の処理能力に対し負担とならない。

【0056】

以上説明したように、本発明の第 1 の実施形態は、適宜の時間間隔毎に設定されたりリモートコピーの一次停止（リモートコピーを一時停止する意味はこの一時停止を境に暗号鍵を変更することである）と一時停止解除との間で暗号鍵を更新し、更新後の暗号鍵をリモートセンタにも通知するシステムであるので、一時停止解除に再開されたりリモートコピーのデータは更新後の暗号鍵を用いてデータ復号されることとなり、リモートセンタへ転送されるデータと暗号鍵との対応付けが明確となっているのである。

【0057】

結局のところ、本発明の第 1 の実施形態は、次のような構成、機能乃至作用を奏するものである。相互に遠隔地に存在するメインセンタのプライマリディスクサブシステム群とリモートセンタのセカンダリディスクサブシステム群とを接続する。メインセンタのプライマリディスクサブシステム群は上位装置より

更新データを受け取ると、自サブシステムへのデータの格納を開始する。

【0058】

そして、プライマリディスクサブシステム群は自サブシステムが暗号鍵を変更するタイミングの状態になっているか否かを確認する。暗号鍵を変更するタイミングの状態になっていない場合は、プライマリディスクサブシステム群は当該データを現在の暗号鍵を用いたりモートセンターへの転送対象とする。暗号鍵を変更するタイミングの状態になっている場合は、今回受けたデータと、今まで受けたデータで未転送分をリモートセンターへ送った後、プライマリディスクサブシステム群はリモートセンターへのデータ転送を一時停止し、暗号鍵を更新し、且つ更新された暗号鍵をリモートセンターへ転送して、一時停止されたりモートセンターへのデータ転送を再開する。

【0059】

前記一時停止の期間はリモートセンターへのデータ転送は行なわない。プライマリディスクサブシステム群においてリモートセンターへのデータ転送の一時停止状態が解除された後は、メインセンターのプライマリディスクサブシステム群はリモートセンターのセカンダリディスクサブシステム群へ更新された暗号鍵を用いてデータ転送を再開する。

【0060】

このようにして、メインセンターとリモートセンターの間で、暗号鍵を更新しながら、リモートコピーによりデータの二重化を行なう。

【0061】

次に、本発明の第2の実施形態として、データの二重化方法と運用の概略を図4を用いて説明する。

【0062】

図4のフローにおいてステップ21～24は、図2のフローのステップ1～4と共通である。ここではステップ25から説明する。

【0063】

上位装置1からライトコマンドを受領した際、プライマリディスクサブシステム3-1、3-2、……3-nは、プライマリディスクサブシステム群3のり

モートコピー制御情報格納部 27 に格納されているリモートコピー状態を表す制御ビットを取得・参照することにより、プライマリディスクサブシステム群 3 が暗号鍵を更新するタイミングにあるか否かを確認する（ステップ 25）。プライマリディスクサブシステム 3-1、3-2、……3-n はプライマリディスクサブシステム群 3 が暗号鍵を更新するタイミングにある場合、暗号鍵を更新する（ステップ 26）。

【 0 0 6 4 】

この後、プライマリディスクサブシステム群 3 からセカンダリディスクサブシステム群 7 に一般的に転送しているデータと同様に、更新された暗号鍵に順序番号（データ順序番号に対応）を付与し（ステップ 27）、この暗号鍵をセカンダリディスクサブシステム 7-1、7-2、……7-n に転送して（ステップ 28）、データの更新位置を示す情報（例えば、データバッファのアドレス）をサブシステム内に保存して（ステップ 29）、書き込みが終了すると上位装置 1 に対しライトコマンドに対する処理の完了を報告する（ステップ 30）。更に、プライマリディスクサブシステム 3-1、3-2、……3-n はプライマリディスクサブシステム群 3 の暗号鍵を更新するタイミングを解除する（ステップ 31）。

【 0 0 6 5 】

以上のことがらを具体的に説明する。ホストから書込み要求（書込みデータ）が送られてくると、プライマリディスクサブシステムは、データが送られてきた順序で、データに順序番号を付与しつつバッファに格納する。これらのデータは適当な契機によって、現在の暗号鍵（旧暗号鍵）を用いて暗号化され、セカンダリディスクサブシステムへ順序番号と共に転送される。この際、セカンダリディスクサブシステムへ転送されるデータの順序は必ずしもホストから送られてきた順序で無くても良い。理由は、セカンダリディスクサブシステムでデータに付与された順序番号に基づいてデータを順番に並び替えることができるからである。

【 0 0 6 6 】

そのうち、暗号鍵の更新タイミングになると、プライマリディスクサブシステムは、自システムの暗号鍵を更新し（新暗号鍵）、且つ、ホストからの書込みデ

ータに付与していた順序番号を採番して、この順序番号を共に更新した暗号鍵をセカンダリディスクサブシステムへ送信する。具体的には、今までデータに順序番号①、②、③が付与されていたとすると、暗号鍵の更新のタイミングで順序番号④を、更新した暗号鍵に与える。

【 0 0 6 7 】

そして、更新した暗号鍵（新暗号鍵）と順序番号④をペアにしてセカンダリディスクサブシステムへ転送する。これを受けたセカンダリディスクサブシステムは、その後、順序番号④を境に更新された暗号鍵を受信データに対して使用する。見方を変えれば、セカンダリディスクサブシステムは、③以下の順序番号を有するデータに対しては更新前の暗号鍵を用いてデータを復号し、⑤以上の順序番号に対しては更新後の暗号鍵を用いてデータを復号する。

【 0 0 6 8 】

その後、プライマリディスクサブシステムは、新たな書込み要求を受けると、順序番号④は既に暗号鍵を送るのに用いているので、この書込み要求のデータに対しては順序番号⑤を与え、バッファに格納する。その後、適当な契機で更新した暗号鍵によってデータを暗号化し、順序番号⑤とともにセカンダリディスクサブシステムへ転送する。

【 0 0 6 9 】

セカンダリディスクサブシステムは、実際のデータを受信すると、受信データを順序番号に従って整列する。そして、順序番号④のところで暗号鍵が更新されていることを知っているセカンダリディスクサブシステムは、順序番号①②③を有するデータに関しては旧暗号鍵を対応させ、順序番号⑤を有するデータに関しては新暗号鍵を対応させ、必要に応じて復号を行う。

【 0 0 7 0 】

また、プライマリディスクサブシステム群 3 が暗号鍵を更新するタイミングにない場合は、プライマリディスクサブシステム 3-1、3-2、……、3-n は、書き込みが終了すると上位装置 1 に対しライトコマンドに対する処理の完了を報告し(ステップ 3 2)、自己のサブシステムの処理能力に基づいて決定された契機で、ライトコマンドをセカンダリディスクサブシステム 7-1、7-2、…

…… 7 - n に対し発行する。そして、現在の暗号鍵でデータは暗号化され、リモートセンタへ転送される。

【 0 0 7 1 】

この時メインセンタにおいて更新が行なわれたデータについて、リモートセンタへライトコマンドを直ちに発行しない場合があるが、これはリモートセンタへ未転送のデータの格納位置情報と共に自サブシステム内に保持される。また、メインセンタにおいて以前に更新が行なわれたデータについて、リモートセンタに未転送のデータの格納位置情報を保持している場合は、当該位置のデータもリモートセンタのセカンダリディスクサブシステム 7 - 1、7 - 2、…… 7 - n への転送対象と判断し、当該データを書込む為のライトコマンドを発行する（ステップ 3 3）。そして、現在の暗号鍵で当該データは暗号化され、リモートセンタへ転送される。当該データの格納位置情報は、ライトコマンドに対する処理が完了した後に、これを消去する。

【 0 0 7 2 】

即ち、プライマリディスクサブシステム群 3 が暗号鍵を更新するタイミングになれば、メインセンタ 9 のプライマリディスクサブシステム群 3 は更新された暗号鍵をリモートセンタ 1 0 のセカンダリディスクサブシステム群 7 に転送する。また、プライマリディスクサブシステム群 3 が暗号鍵を更新するタイミングになれば、メインセンタ 9 のプライマリディスクサブシステム群 3 は上位装置 1 からライトコマンドが発行される事に起因しリモートコピーが実施される。

【 0 0 7 3 】

セカンダリディスクサブシステム 7 - 1、7 - 2、…… 7 - n は、プライマリディスクサブシステム 3 - 1、3 - 2、…… 3 - n から発行されたライトコマンドを受領していることを確認すると、ライトコマンドに対する処理、即ち、自己のサブシステム内のデータバッファ 2 2 へのデータ格納処理を行なう（ステップ 3 4）。

【 0 0 7 4 】

セカンダリディスクサブシステム 7 - 1、7 - 2、……、7 - n は、ライトコマンドに対する処理、即ち、自己のサブシステム内のデータバッファ 2 2 への

データ格納処理が完了すると、プライマリディスクサブシステム 3-1、3-2、……3-n に対し、ライトコマンドに対する処理完了報告を行なう（ステップ 35）。

【0075】

本発明により、上位装置 1 から書込まれたデータは、プライマリディスクサブシステム 3-1、3-2、……、3-n に格納されるだけでなく、セカンダリディスクサブシステム 7-1、7-2、7-n にも複写され格納される。また、プライマリディスクサブシステム群 3 が暗号鍵を更新するタイミングとなった時点で、プライマリディスクサブシステム群 3 が更新された暗号鍵に順序番号を付与して、セカンダリディスクサブシステム群 7 に転送する。

【0076】

セカンダリディスクサブシステム群 7 は、プライマリディスクサブシステム群 3 が一般的に転送しているデータ及び更新された暗号鍵に付与した順序番号を使用して、当該更新された暗号鍵を適用すべきデータを特定して復号することが出来る。メインセンター 9 が被災した場合は、セカンダリディスクサブシステム 7-1、7-2、……7-n のデータを利用して、ジョブを再実行する等の回復作業を行い、業務を再開する。これらはすべてディスクサブシステムの機能のみで実現され、上位装置の処理能力に対し負担とならない。

【0077】

次に、本発明の第 3 の実施形態として、データの二重化方法と運用の概略を図 5 を用いて説明する。ここでは、セカンダリディスクサブシステムは、プライマリディスクサブシステムから受けた暗号化されたデータを、そのまま記憶しているものとする。

【0078】

リモートコピー実行中にメインセンター 9 に災害が発生した（ステップ 41）場合の動作である。メインセンター 9 は災害が発生したことをリモートセンター 10 に通知する（ステップ 42）。これに対して、リモートセンター 10 は、システム立上げ等の災害回復を開始する（ステップ 43）。復号することなくリモートセンター 10 のセカンダリディスクサブシステム群 7 に記憶されていたデー

タを利用に供するために、暗号の復号を開始する（ステップ44）。この時、暗号鍵をセカンダリディスクサブシステム群7に記憶している場合は、その暗号鍵を使用して復号する。暗号鍵はリモートセンター10以外の別の場所にある記憶装置に記憶することも出来る。この場合は、その暗号鍵をリモートセンター10のセカンダリディスクサブシステム群7に転送して、これを使用して復号する。

【0079】

リモートセンター10の上位装置8からセカンダリディスクサブシステム群7のデータに対してアクセスがある（ステップ45）と、セカンダリディスクサブシステム群7はアクセスされたデータが復号済か否かを調べる（ステップ46）。アクセスされたデータが復号済でない場合、セカンダリディスクサブシステム群7はそのデータに関して暗号の復号を実行し（ステップ47）、復号されたデータを使用してアクセスに応答する（ステップ48）。アクセスされたデータが復号済である場合、セカンダリディスクサブシステム群7はそのデータを使用してアクセスに応答する（ステップ48）。これらはすべてディスクサブシステムの機能のみで実現され、上位装置の処理能力に対し負担とならない。

【0080】

このように、メインセンターに災害が発生した場合には、リモートセンターにおけるコピーデータは、メインセンターに依拠せずに、リモートセンターのディスクサブシステムによって、メインセンターに代わって、利用に供されるようにコピーデータの全て又は適宜にアクセスされたコピーデータについてデータ復号されるのである。

【0081】

次に、本発明の第4の実施形態として、データの二重化方法と運用の概略を図6を用いて説明する。

【0082】

リモートコピーされて復号することなくリモートセンター10のセカンダリディスクサブシステム群7に記憶されていたデータを利用に供するために、リモートセンター10からセカンダリディスクサブシステム群7にアクセスする（ステップ51）場合の動作である。一般にデータに対するアクセスはそのデータに関

連する I D フィールドあるいはキーフィールドを搜索して搜索条件が成立した場合に以降のデータが読出し／書込みされる。

【 0 0 8 3 】

この時、特定のフィールド、例えばキーフィールドに対する搜索条件が成立するか否かを調べる（ステップ 5 2）。この条件が成立した場合は、以降のデータが復号されて（ステップ 5 3）、読出し／書込みされる（ステップ 5 4）。この条件が成立しない場合は、以降のデータが復号されることなく、エラー報告される（ステップ 5 5）。これらはすべてディスクサブシステムの機能のみで実現され、上位装置の処理能力に対し負担とならない。

【 0 0 8 4 】

【発明の効果】

上位装置への新規ソフトウェアの導入を必要とせずサブシステム側の機能変更のみで、ユーザが期待する範囲での更新データの一貫性を保証出来、かつ暗号鍵の更新により情報漏洩の危険性を低減出来る、リモートコピーの暗号化システムを実現出来る。

【図面の簡単な説明】

【図 1】

本発明の一実施形態に係るリモートコピーのコンピュータシステムの全体構成を示す図である。

【図 2】

リモートコピーシステムの処理を示すフローチャートである。

【図 3】

本実施形態に関するメインセンターのプライマリディスクサブシステムの構成を示す図である。

【図 4】

リモートコピーシステムの処理を示すフローチャートである。

【図 5】

リモートコピーシステムの処理を示すフローチャートである。

【図 6】

リモートコピーシステムの処理を示すフローチャートである。

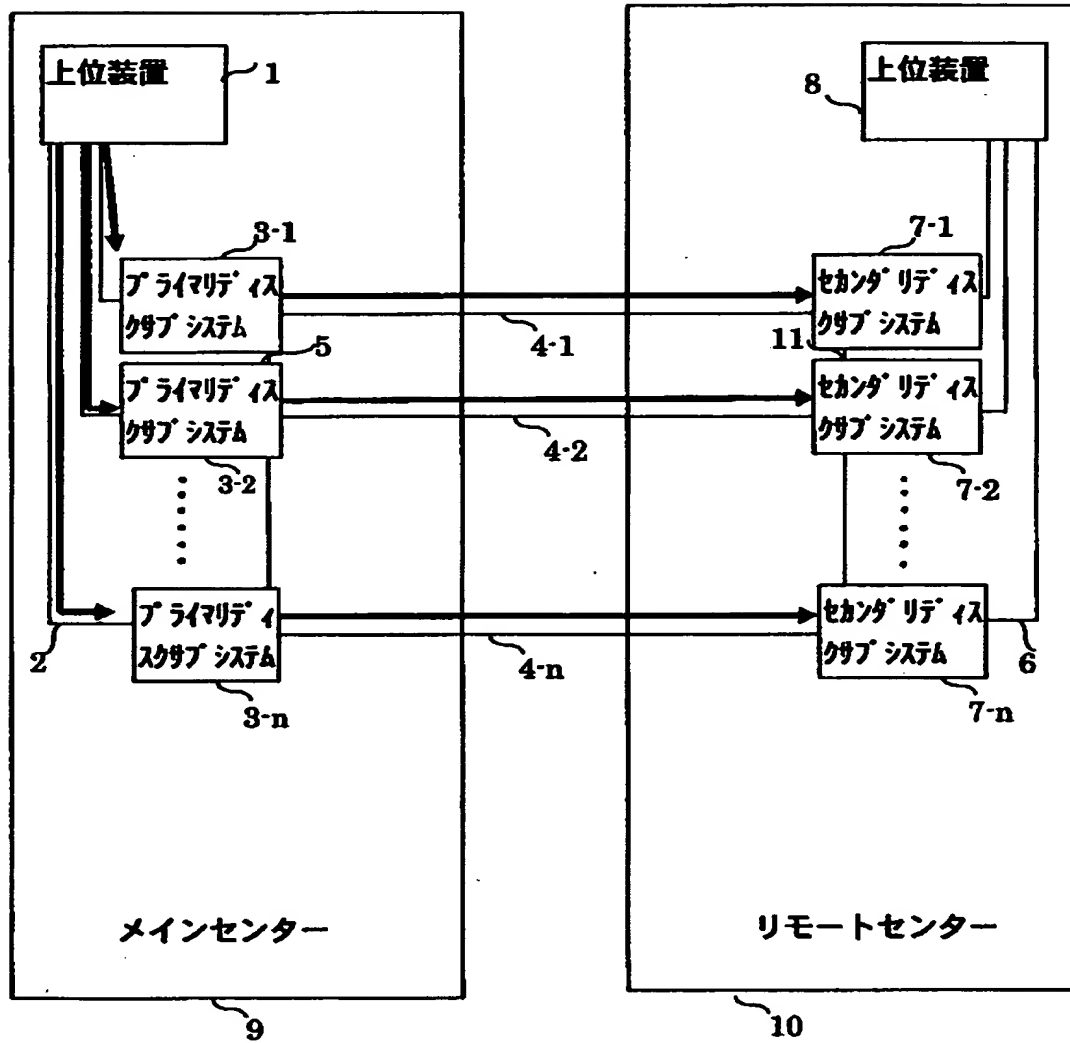
【符号の説明】

- 1 上位装置
- 2 インタフェースケーブル
- 3 プライマリディスクサブシステム
- 4 インタフェースケーブル
- 5 インタフェースケーブル
- 6 インタフェースケーブル
- 7 セカンダリディスクサブシステム
- 8 上位装置
- 9 メインセンター
- 10 リモートセンター
- 11 インタフェースケーブル
- 21 インタフェース制御部
- 22 データバッファ
- 23 磁気ディスクドライブ
- 24 マイクロプロセッサ
- 25 ディスクアレイサブシステム制御部
- 26 コンソール
- 27 リモートコピー制御情報格納部

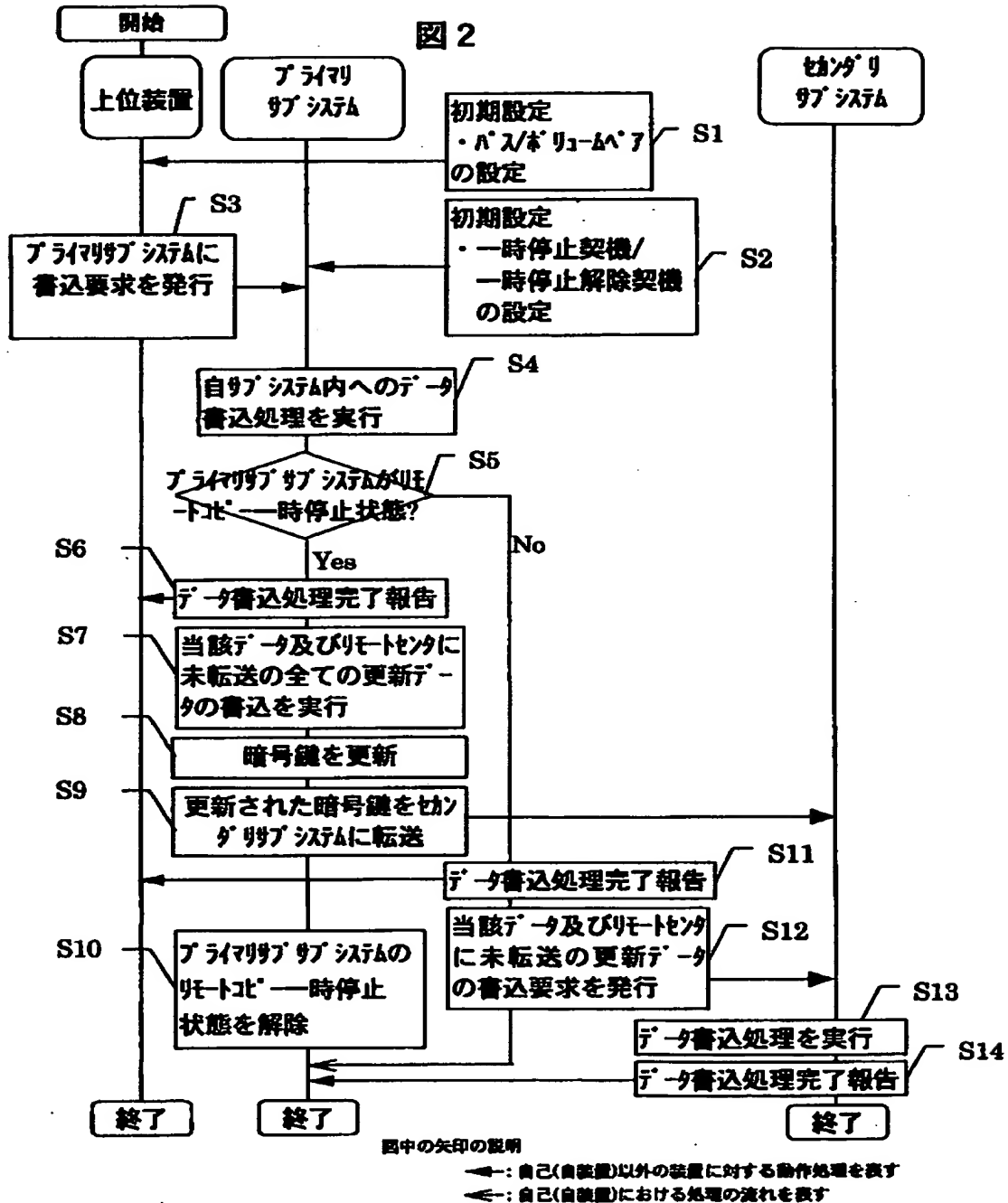
【書類名】 図面

【図 1】

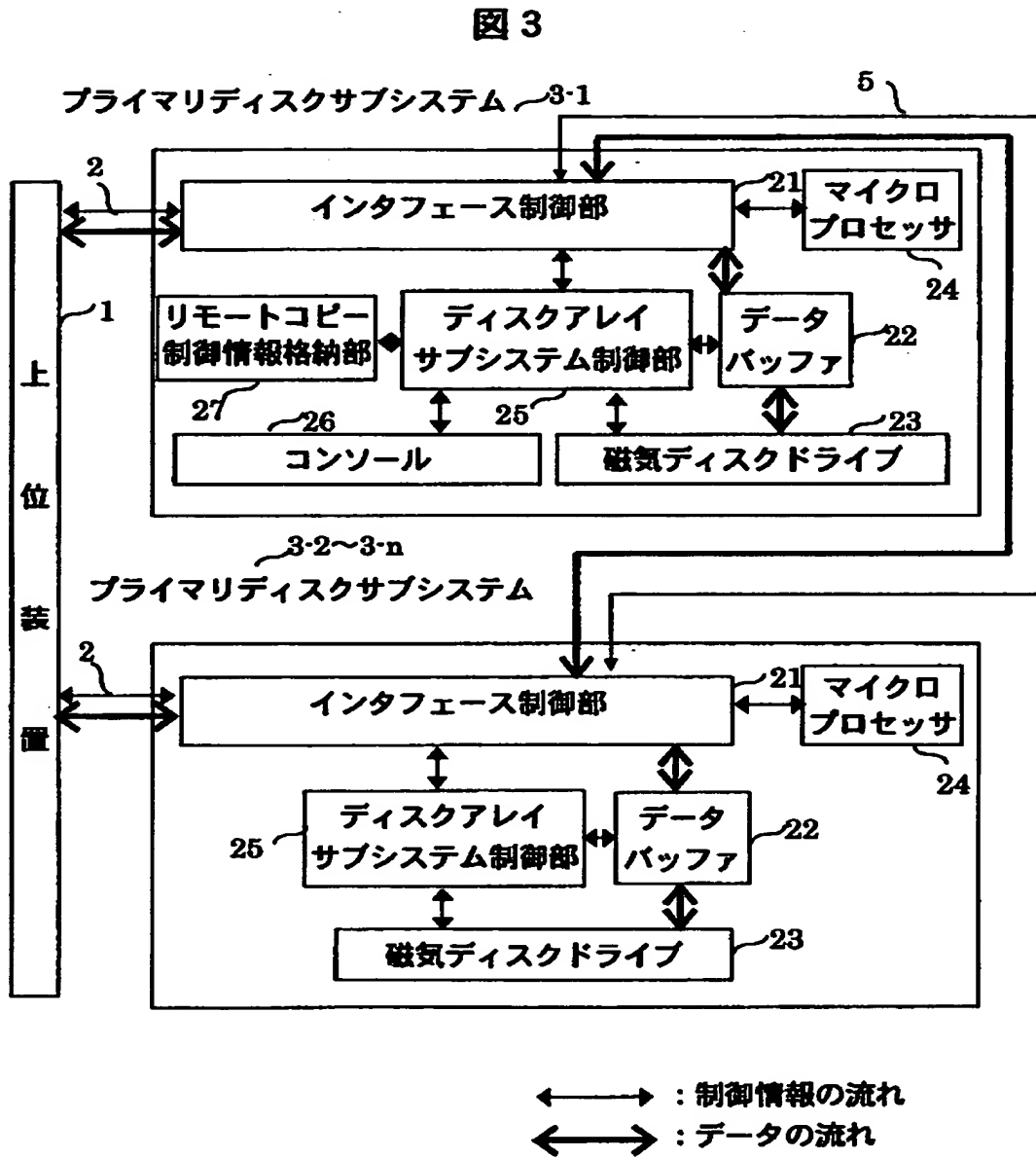
図 1



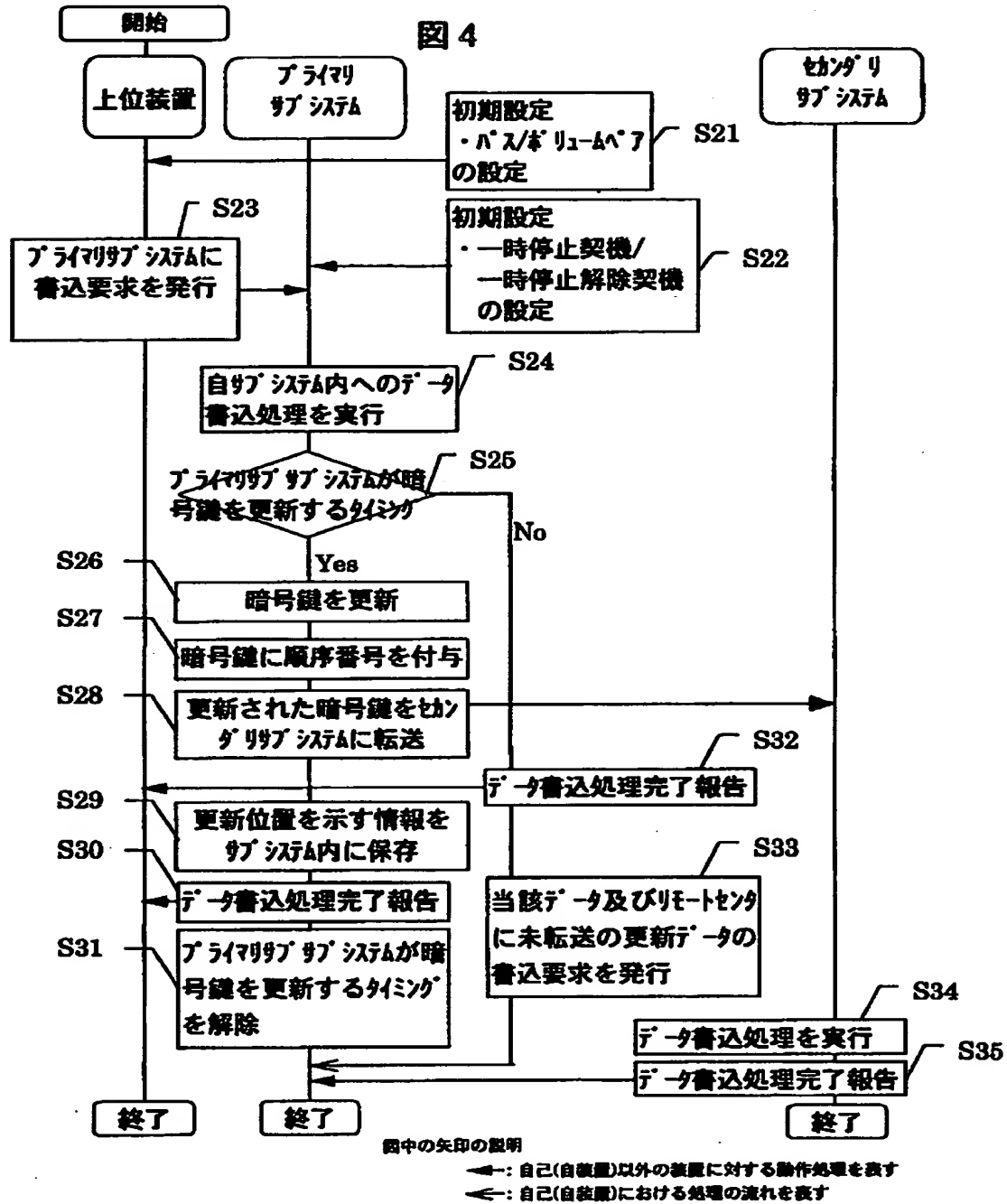
【図 2】



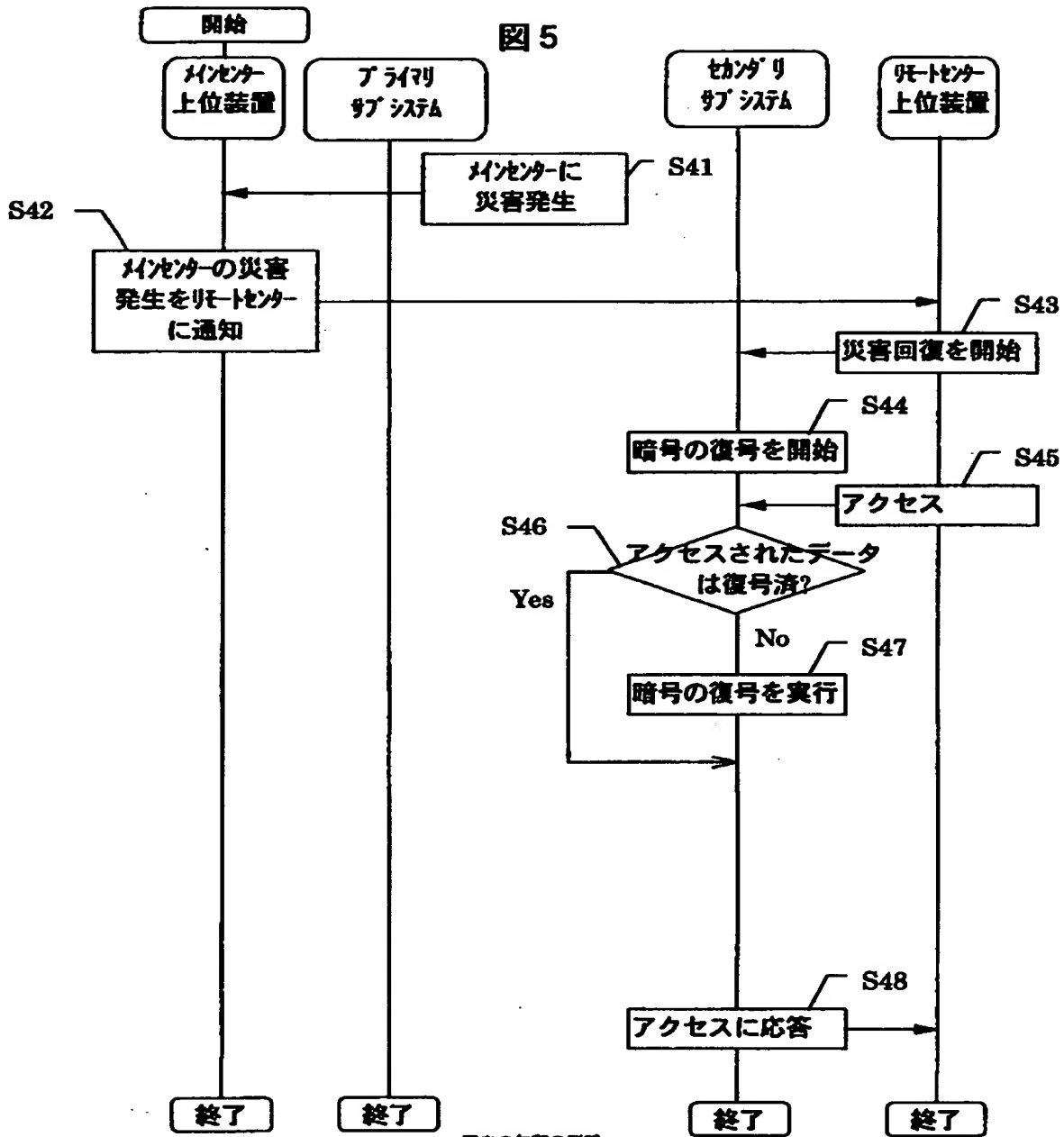
【図3】



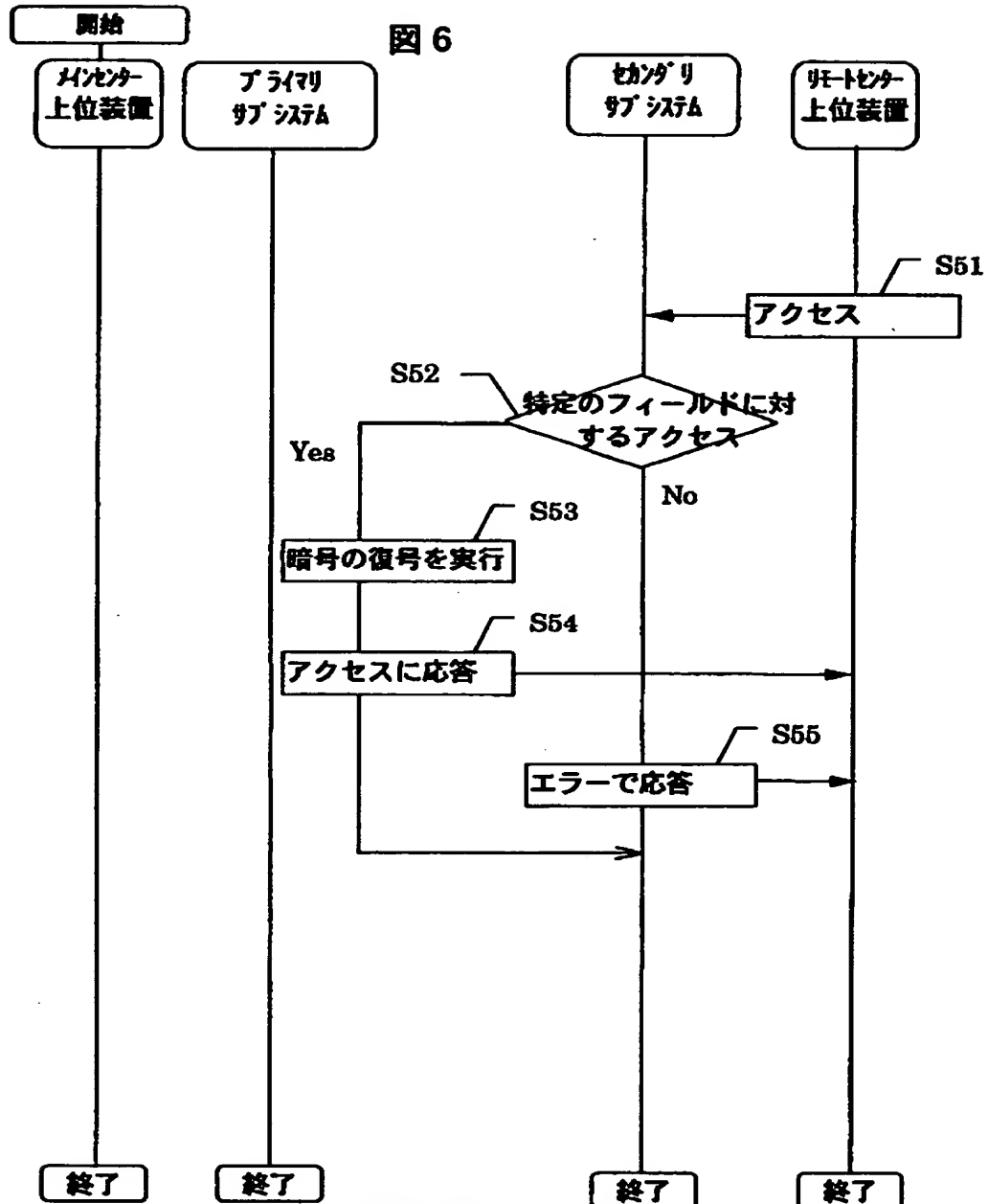
【図 4】



【図5】



【図 6】



図中の矢印の説明

- ←: 自己(自装置)以外の装置に対する動作処理を表す
- : 自己(自装置)における処理の流れを表す

【書類名】 要約書

【要約】

【課題】 高いデータ転送性能と高い暗号強度とを両立させたりモートコピー機能を提供する。

【解決手段】 メインセンター 9 では、予め設定された契機でプライマリディスクサブシステム群 3 がリモートコピーの一時停止停止と一時停止解除を反復し、これに連動してプライマリディスクサブシステム群 3 が暗号鍵をリモートセンター 10 のセカンダリディスクサブシステム群 7 に転送することでメインセンター 9 とリモートセンター 10 の暗号鍵の更新を行なう。また、予め設定された契機でプライマリディスクサブシステム群 3 が暗号鍵を更新するタイミングと暗号鍵を更新するタイミングの解除を反復し、これに連動してプライマリディスクサブシステム群 3 が暗号鍵をリモートセンター 10 のセカンダリディスクサブシステム群 7 に転送することでメインセンター 9 とリモートセンター 10 の暗号鍵の更新を行なう。

【選択図】 図 2

出 願 人 履 歴 情 報

識別番号 {000005108}

1. 変更年月日 1990年 8月31日
[変更理由] 新規登録
住 所 東京都千代田区神田駿河台4丁目6番地
氏 名 株式会社日立製作所